Appl. No. 09/937,634 Amdt. dated March 20, 2006 Reply to Office Action of December 21, 2005

AMENDMENT TO THE SPECIFICATION

Please replace the paragraph beginning on Line 20 of Page 5 of the specification with the following paragraph:

FIGURE 1 shows the operation of the present invention at the encrypting end of a communication channel. Data encryption is performed using two cryptographic algorithms, the first being a cryptographic pseudo random sequence generator R() which is a sequence generating function and the second being a high-speed cipher E() which is functionally a ciphering function. The high-speed cipher, which may be relatively weak in security when used alone. The pseudo random sequence generator accepts two inputs k and ν and outputs a pseudo random sequence $s = R(k, \nu)$. The high-speed cipher accepts a secret key s and a data segment d and produces the ciphertext c = E(s, d). In addition, the illustrative embodiment uses a predetermined function F() to update an initial value, i. e., $\nu_i = F(V_{i-1})$. It is assumed that the encrypting end and decrypting ends share a secret key k, an initial value ν_0 , and the functions F() and R(). Moreover, it is assumed that the decrypting end knows the decrypting algorithm D() corresponding to the encrypting algorithm E().